Pandu Ranga Reddy Konala

Bengaluru, Karnataka

pandurangareddy414@gmail.com | pandukonala.github.io

Personal Statement

Cybersecurity researcher focused on securing the intersection of AI code generation and modern DevSecOps practices. My PhD research develops frameworks for detecting vulnerabilities in Infrastructure as Code, from misconfigurations to supply chain attacks, through metadata-driven analysis of security smell diffusion patterns. Applied to AI-generated code, my zero-shot evaluation methods achieve 100% CIS benchmark compliance compared to 23% for human-written code. I'm seeking opportunities to advance cybersecurity research and develop scalable approaches for securing modern software development practices.

Academic Progress

The University of Waikato — *Hamilton, New Zealand*

PhD in Computer Science — *April 2022 - January 2026*

- Fully funded by MBIE, New Zealand, through the AI for Human-Centric Security Catalyst project scholarship
- Research Topic: A Code Quality Framework for Infrastructure as Code in the Modern DevSecOps Era

Lancaster University — *Lancaster, United Kingdom*

Masters in Cyber Security — *September 2019 - September 2020*

- Fully funded by Lancaster University through the Cyber Security Scholarship program
- Certified by the National Cyber Security Centre (NCSC), UK

Amrita Vishwa Vidyapeetham — *Coimbatore, India*

Bachelor of Technology in Computer Science and Engineering — *June 2015 - April 2019*

- Specialized in Cyber Security

Work Experience

Research Associate — *Hamilton, New Zealand*

School of Computing & Mathematical Sciences, The University of Waikato — *February 2021 - January 2026*

- Conducting experiments and contributing to cybersecurity-related research activities.
- Providing comprehensive support to faculty and students in research projects and academic activities.

Software Developer — *Lancaster, UK*

Quantum Base — *June 2020 - September 2020*

- Designed and implemented secure system architectures to integrate quantum PUFs with IoT devices, bridging the gap between quantum technology and everyday applications.

Security Analyst Intern — *Lucknow, India*

Infosec Future Pvt Ltd — *May 2018 - June 2018*

- Conducted website penetration testing, vulnerability scanning, and risk analysis using automated tools and manual techniques during an eight-week internship.
- Performed detailed information gathering to identify security risks and vulnerabilities.

Red Hat System Administrator Intern — *Hyderabad, India*

Complete Open Source Solutions (COSS) — *May 2017 - June 2017*

- Gained hands-on experience in managing and maintaining Red Hat Enterprise Linux systems during a four-week internship.
- Handled system installation, configuration, performance monitoring, security management and maintained system documentation.

Ethical Hacker Intern — *Vizag, India*

Star Computers — *May 2016 - May 2016*

- Gained hands-on experience in penetration testing and vulnerability assessments over a four-week period.
- Identified potential vulnerabilities and security risks in client systems and applications through various tests and assessments.

Professional Certifications

Red Hat Certified Engineer (RHCE) by Red Hat, License No. 170-138-911 (2017 - 2020)

Red Hat Certified System Administrator (RHCSA) by Red Hat, License No. 170-138-911 (2017 - 2020)

Certified Ethical Hacker (CEH) by EC-Council, License No. ECC022209621222 (2016 - 2019)

Skills

Cyber Security Tools Metasploit Framework, Nessus, Burp Suite & Other Cyber Security Tools

Programming Python, Java, R, HTML/CSS, SQL, Node.js

Operating Systems Red Hat Linux, Kali, Debian

Virtualization Technologies VMware vSphere, Containers (Docker)

Miscellaneous LaTeX(Overleaf/ Markdown), Tableau, Microsoft Office, Power Automate, Git, Hack The Box

Peer-Reviewed Research Publications

Tracking Security Smell Diffusion Patterns in Ansible Playbooks Using Metadata *Published*
Research Paper (First-Author) *November 2025*
- International Workshop on Security (IWSEC) 2025, Japan

Metadata Assisted Supply-Chain Attack Detection for Ansible *Published*
Research Paper (First-Author) *June 2025*
- Conference on Data and Applications Security and Privacy (DBSec), Norway

SoK: Static Configuration Analysis in Infrastructure as Code Scripts *Published*
Research Paper (First-Author) *August 2023*
- IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy

Access mechanism using inter planetary file system *Published*
Research Paper (First-Author) *April 2019*
- International Journal of Engineering and Technology, Volume 7, No 4, ISSN: 2227-524X

Securing Data in Cloud- A Physical Cyber System *Published*
Research Paper (First-Author) *December 2017*
- Journal of Computer Science Engineering, Volume-3, Issue-12, ISSN-2456-1843

A Policy-Driven Framework for Measuring the Code Quality of Ansible Roles: An Empirical Study *Under Review*
Research Paper (First-Author) *2026*
- Journal of Systems and Software (JSS)

Evaluating and Preventing Security Smells in AI-Generated Ansible Code *Under Review*
Research Paper (First-Author) *2026*
- IFIP Information Security & Privacy Conference (SEC), Australia

Projects

AI for Human Centric Security | MBIE Catalyst Project *PhD Project*
The University of Waikato *April 2022 - January 2026*
- Developed a policy-driven code quality framework for Infrastructure as Code that detects simple vulnerabilities and complex threats such as supply chain attacks, performs advanced metadata-driven analysis to identify hidden security smell diffusion pathways, and evaluates AI-generated code quality and security using zero-shot approaches achieving 100% CIS security benchmark compliance versus 23.8% for human-written code.

Cryptographically Secure On-Line Identity System *Masters Project*
Lancaster University *June 2020 - September 2020*
- Funded by Quantum Base and The Royal Society, UK, this project developed a framework leveraging quantum computer-generated identities (PUFs) for device authentication and validation, targeting resource-constrained devices like IoT and mobile applications.

Secure communication using IPFS with IoT *Under Graduate Project*
Amrita Vishwa Vidyapeetham *June 2018 - April 2019*
- Funded by Amrita Vishwa Vidyapeetham, this project utilized the Interplanetary File System (IPFS) web3 protocol for secure, direct communication between users and IoT devices, eliminating the need for third-party vendors.

Crop Prediction System using Machine Learning algorithm *Industry Project*
Amrita Vishwa Vidyapeetham *June 2017 - December 2017*
- Funded by Amrita Vishwa Vidyapeetham, this project developed a K-Means-based Crop Prediction System to provide farmers with recommendations based on soil type, location, and sowing time.

Voluntary Activities

New Zealand Cyber Security Challenge *cybersecuritychallenge.org.nz*
2022 - 2025
- Organized and facilitated Capture The Flag (CTF) events for the New Zealand Cyber Security Challenge, engaging over 500 participants, including high school students, university students, and industry professionals, to enhance their cybersecurity skills and awareness.

Cyber Security Workshop *Amrita School of Engineering, India*
February 2016
- Organized and led a two-day workshop on Ethical Hacking and Cyber Security at Amrita School of Engineering, India, aimed at inspiring students from underprivileged backgrounds to explore opportunities in cybersecurity.

Interests

Hack The Box Active participant in Hack The Box challenges, honing penetration testing, problem-solving, and cybersecurity skills.

Travel Passionate about traveling and exploring diverse cultures & learning about history, which has broadened my perspective and enriched my understanding of the world.

Video Games Enthusiastic about gaming, particularly exploring immersive stories and unique experiences that games offer.

Swimming Avid professional swimmer since the age of 10, fascinated by underwater exploration and challenges requiring breath control.